CLAIMS

What is claimed is:

1. A method, comprising:

in an operating system environment controlled by a single operating system kernel instance, establishing a global zone and at least one non-global zone for isolating processes from processes in other non-global zones;

receiving from a first process executing in association with the non-global zone a first request to perform an operation;

in response to receiving the first request, determining whether performing the requested operation enables the first process to obtain additional privileges for which the first process is not authorized; and

denying the first request if the first process is enabled to obtain the additional privileges.

2. The method of claim 1, wherein each non-global zone has a set of allowable privileges for processes executing within the non-global zone.

3. The method of claim 2, wherein the operation comprises obtaining control of a second process, and wherein determining whether performing the requested operation enables the first process to obtain the additional privileges comprises:

determining if a zone identifier of the first process matches with a zone identifier of a second process; and

if the zone identifiers do not match, determining if the first process is associated with a non-global zone; and if so, denying the request;

otherwise, determining if the first process has a privilege to control processes in other zones; and

if the first process does not have the privilege to control processes in other zones, denying the request;

determining if a user identifier of the first process matches with a user identifier of a second process; and

if the user identifiers do not match, determining if the first process has a process owner privilege; and

if the first process does not have the process owner privilege, denying the request;

determining if the first process has at least each of the privileges possessed by the second process; and

if the first process does not have each of the privileges of the second process, denying the request;

determining if the user identifier of the second process is a privileged user identifier; and

if the second process does not have a privileged user identifier, permitting the request;

determining if the first process is associated with the global zone; and

if the first process is a global zone process, then determining if the first process has all privileges; and

if so, permitting the request; otherwise, denying the request;

otherwise, if the first process is associated with a non-global zone, then

determining if the first process has all privileges in the set of allowable privileges for the non-global zone; and

if so, permitting the request; otherwise, denying the request.

4. The method of claim 3, wherein the privileged user identifier is 0.

5. The method of claim 2, wherein establishing a non-global zone for isolating processes from processes in other non-global zones, comprises:

setting a privilege limit for the non-global zone, the privilege limit indicating the set of allowable privileges for processes executing within the non-global zone.

6. The method of claim 5, wherein the privilege limit is represented as a bit mask passed to the non-global zone when created, the method further comprising:

comparing privileges held by a process joining the non-global zone against the bit mask; and

removing any privileges not in the bit mask from the process.

7. The method of claim 1, wherein performing the requested operation comprises accessing an object, the method further comprising:

determining whether the first process has permission to access the object.

8. The method of claim 1, wherein the operation includes one of:

(un)mounting a file system, overriding file system permissions, binding to a privileged network port, and controlling other processes with different user identifiers.

9. The method of claim 2, wherein the operation comprises changing a user identifier associated with the first process, and wherein determining whether performing the requested operation enables the first process to obtain the additional privileges comprises:

determining if the request is to change the user identifier associated with the first process to a privileged user identifier, and if the first process has at least each of the privileges in the set of allowable privileges for the non-global zone; and

if so, granting the request;

otherwise, determining if the first process has a privilege appropriate for the request; and,

if so, granting the request;

otherwise, denying the request.

10. The method of claim 1, further comprising:

receiving from a process executing in association with the global zone a request to perform an operation;

in response to receiving the request, determining whether performing the requested operation enables the process to obtain additional privileges for which the process is not authorized; and

denying the request if the process is enabled to obtain the additional privileges.

11. The method of claim 10, wherein the operation comprises obtaining control of a second process, and wherein determining whether performing the requested operation enables the process executing in association with the global zone to obtain the additional privileges comprises:

determining if a zone identifier of the first process matches with a zone identifier of a second process; and

if the zone identifiers do not match, determining if the first process is associated with a non-global zone; and if so, denying the request;

otherwise, determining if the first process has a privilege to control processes in other zones; and

if the first process does not have the privilege to control processes in other zones, denying the request;

determining if a user identifier of the first process matches with a user identifier of a second process; and

if the user identifiers do not match, determining if the first process has a process owner privilege; and

if the first process does not have the process owner privilege, denying the request;

determining if the first process has at least each of the privileges possessed by the second process; and

if the first process does not have each of the privileges of the second process, denying the request;

determining if the user identifier of the second process is a privileged user identifier; and

if the second process does not have a privileged user identifier, permitting the request;

determining if the first process is associated with the global zone; and

if the first process is a global zone process, then determining if the first process has all privileges; and

if so, permitting the request; otherwise, denying the request;

otherwise, if the first process is associated with a non-global zone, then determining if the first process has all privileges in the set of allowable privileges for the non-global zone; and

if so, permitting the request; otherwise, denying the request.

12. The method of claim 10, wherein the operation comprises changing a user identifier associated with the process executing in association with the global zone, and wherein determining whether performing the requested operation enables the process executing in association with the global zone to obtain the additional privileges comprises:

determining if the request is to change the user identifier associated with the process executing in association with the global zone to a privileged user identifier, and if the process executing in association with the global zone has all privileges; and

if so, granting the request;

otherwise, determining if the process executing in association with the global zone has a privilege appropriate for the request; and,

if so, granting the request;

otherwise, denying the request.

13. The method of claim 10, wherein the operation includes one of:

modifying all process privileges, writing to system administration file, opening device holding kernel memory, modifying operating system code, accessing file systems restricted to root user, setting the system clock, changing scheduling priority of an executing process, reserving resources for an application, directly accessing a network layer and loading kernel modules.

14. A computer readable medium, comprising instructions for causing one or more processors to perform the steps of:

establishing a global zone and at least one non-global zone for isolating processes from processes in other non-global zones in an operating system environment controlled by a single operating system kernel instance;

receiving from a first process executing in association with the non-global zone a first request to perform an operation;

in response to receiving the first request, determining whether performing the requested operation enables the first process to obtain additional privileges for which the first process is not authorized; and

denying the first request if the first process is enabled to obtain the additional privileges.

15. The computer readable medium of claim 14, wherein each non-global zone has a set of allowable privileges for processes executing within the non-global zone.

16. The computer readable medium of claim 15, wherein the operation comprises obtaining control of a second process, and wherein determining whether performing the requested operation enables the first process to obtain the additional privileges comprises:

determining if a zone identifier of the first process matches with a zone identifier of a second process; and

if the zone identifiers do not match, determining if the first process is associated with a non-global zone; and if so, denying the request;

otherwise, determining if the first process has a privilege to control processes in other zones; and

if the first process does not have the privilege to control processes in other zones, denying the request;

determining if a user identifier of the first process matches with a user identifier of a second process; and

if the user identifiers do not match, determining if the first process has a process owner privilege; and

if the first process does not have the process owner privilege, denying the request;

determining if the first process has at least each of the privileges possessed by the second process; and

if the first process does not have each of the privileges of the second process, denying the request;

determining if the user identifier of the second process is a privileged user identifier; and

if the second process does not have a privileged user identifier, permitting the request;

determining if the first process is associated with the global zone; and

if the first process is a global zone process, then determining if the first process has all privileges; and

if so, permitting the request; otherwise, denying the request;

otherwise, if the first process is associated with a non-global zone, then determining if the first process has all privileges in the set of allowable privileges for the non-global zone; and

if so, permitting the request; otherwise, denying the request.

17. The computer readable medium of claim 16, wherein the privileged user identifier is 0.

18. The computer readable medium of claim 15, wherein establishing a non-global zone for isolating processes from processes in other non-global zones, comprises:

setting a privilege limit for the non-global zone, the privilege limit indicating the set of allowable privileges for processes executing within the non-global zone.

19. The computer readable medium of claim 18, wherein the privilege limit is represented as a bit mask passed to the non-global zone, the computer readable medium further comprising instructions for causing one or more processors to perform the steps of:

comparing privileges held by a process joining the non-global zone against the bit mask; and

removing any privileges not in the bit mask from the process.

20. The computer readable medium of claim 14, wherein performing the requested operation comprises accessing an object, the computer readable medium further comprises instructions for causing one or more processors to perform the step of:

determining whether the first process has permission to access the object.

21. The computer readable medium of claim 14, wherein the operation includes one of:

(un)mounting a file system, overriding file system permissions, binding to a privileged network port, and controlling other processes with different user identifiers.

22. The computer readable medium of claim 15, wherein the operation comprises changing a user identifier associated with the first process, and wherein determining whether performing the requested operation enables the first process to obtain the additional privileges comprises instructions for causing one or more processors to perform the steps of:

determining if the request is to change the user identifier associated with the first process to a privileged user identifier, and if the first process has at least each of the privileges in the set of allowable privileges for the non-global zone; and

if so, granting the request;

otherwise, determining if the first process has a privilege appropriate for the request; and,

if so, granting the request;

otherwise, denying the request.

23. The computer readable medium of claim 14, further comprising instructions for causing one or more processors to perform the steps of:

receiving from a process executing in association with the global zone a request to perform an operation;

in response to receiving the request, determining whether performing the requested operation enables the process in the global zone to obtain privileges in addition to privileges associated with the process; and

denying the request if the process is enabled to obtain additional privileges outside of privileges associated with the process.

24. The computer readable medium of claim 23, wherein the operation comprises obtaining control of a second process, and wherein determining whether performing the requested operation enables the process executing in association with the global zone to obtain the additional privileges comprises instructions for causing one or more processors to perform the steps of:

determining if a zone identifier of the first process matches with a zone identifier of a second process; and

if the zone identifiers do not match, determining if the first process is associated with a non-global zone; and if so, denying the request;

otherwise, determining if the first process has a privilege to control processes in other zones; and

if the first process does not have the privilege to control processes in other zones, denying the request;

determining if a user identifier of the first process matches with a user identifier of a second process; and

if the user identifiers do not match, determining if the first process has a process owner privilege; and

if the first process does not have the process owner privilege, denying the request;

determining if the first process has at least each of the privileges possessed by the second process; and

if the first process does not have each of the privileges of the second process, denying the request;

determining if the user identifier of the second process is a privileged user identifier; and

if the second process does not have a privileged user identifier, permitting the request;

determining if the first process is associated with the global zone; and

if the first process is a global zone process, then determining if the first process has all privileges; and

if so, permitting the request; otherwise, denying the request;

otherwise, if the first process is associated with a non-global zone, then determining if the first process has all privileges in the set of allowable privileges for the non-global zone; and

if so, permitting the request; otherwise, denying the request.

25. The computer readable medium of claim 23, wherein the operation comprises changing a user identifier associated with the process executing in association with the global zone, and wherein determining whether performing the requested operation enables the process executing in association with the global zone to obtain the additional privileges comprises instructions for causing one or more processors to perform the steps of:

determining if the request is to change the user identifier associated with the process executing in association with the global zone to a privileged user identifier, and if the process executing in association with the global zone has all privileges; and

if so, granting the request;

otherwise, determining if the process executing in association with the global zone has a privilege appropriate for the request; and,

if so, granting the request;

otherwise, denying the request.

26. The computer readable medium of claim 23, wherein the operation includes one of: modifying all process privileges, writing to system administration file, opening device holding kernel memory, modifying operating system code, accessing file systems restricted to root user, setting the system clock, changing scheduling priority of an executing process, reserving resources for an application, directly accessing a network layer and loading kernel modules.

27. An apparatus, comprising:

means for establishing a global zone and at least one non-global zone for isolating processes from processes in other non-global zones in an operating system environment controlled by a single operating system kernel instance;

means for receiving from a first process executing in association with the non-global zone a first request to perform an operation;

means for determining in response to receiving the first request whether performing the requested operation enables the first process to obtain additional privileges for which the first process is not authorized; and

means for denying the first request if the first process is enabled to obtain the additional privileges.